

# Number of Solutions of Linear Congruence Systems

Marcus Nilsson  
marcus.nilsson@lnu.se  
Linnaeus University  
Sweden

Robert Nyqvist  
robert.nyqvist@bth.se  
Blekinge Institute of Technology  
Sweden

August 20, 2012

## Abstract

## 1 Introduction

We will consider the system of linear congruences,

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n \equiv b_1 \pmod{m} \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n \equiv b_2 \pmod{m} \\ \vdots \\ a_{n1}x_1 + a_{n2}x_2 + \cdots + a_{nn}x_n \equiv b_n \pmod{m}, \end{cases} \quad (1)$$

where  $m, n$  are positive integers, and all  $a_{ij}, b_i$  are integers. We are interested in finding an expression for the number of solutions to this system. Let  $A = (a_{ij})$  denote the coefficient matrix. It is well known that this system has a unique solution if and only if  $\det(A)$  and  $m$  are relatively prime, see for example [8]. But, how many solutions do we have if  $\det(A)$  and  $m$  have a common divisor greater than 1? The authors became interested in this question when they were working on multidimensional  $p$ -adic monomial dynamical systems [7]. The problem was solved by Butson and Stewart, [1], by rewriting the system into Smith normal form. The solvability of linear congruence systems and algorithms for finding a solution have been of interest for many mathematicians and computer scientists over the years. Examples of other contributions to the problem on solving systems of linear congruences can be found in [2], [6], [3], [4] and [9].

Compared to Butson and Stewart we will use a more direct method. We use Gaussian elimination with successive reduction and the Chinese remainder theorem instead of the Smith normal form. We will find a different formula for the number of solutions than in [1]. The algorithm used in the proof of the

formula can with small changes also be used to find all incongruent solutions to the system, since we only have used elementary methods.

The paper is organized as follows: In Section 2 we give definitions and notations together with some theorems about solvability of systems of linear congruences. Section 3 is the main section in which we derive the formula for the number of solutions to homogeneous systems. Applications to inhomogeneous systems are mentioned in Section 4. In Section 5 we present an algorithm in pseudo code for calculating the number of solutions. The algorithm also gives us all the solutions. In Section 6 we discuss generalizations of our results.

## 2 Notations

Two solutions of the linear congruence system (1) are said to be *incongruent modulo  $m$*  if they differ at least in one coordinate modulo  $m$ . We want to find the number of incongruent solutions modulo  $m$  the system have. Let  $A$  denote the coefficient matrix,  $\mathbf{x}$  the vector of the indeterminates, and  $\mathbf{b}$  the vector of the elements on the right hand side in the system, that is,  $A = (a_{ij})$ ,  $\mathbf{x} = (x_1, x_2, \dots, x_n)$  and  $\mathbf{b} = (b_1, b_2, \dots, b_n)$ . Then the system (1) can be written in matrix form as

$$A\mathbf{x} \equiv \mathbf{b} \pmod{m}. \quad (2)$$

Let  $\eta(A, \mathbf{b}, m)$  denote the number of incongruent solutions modulo  $m$  to the congruence (2).

Let  $\text{adj}(A)$  denote the adjoint matrix of a square matrix  $A$  over order  $n$ . It is known from linear algebra that  $\text{adj}(A)$  has the following properties:

$$\det(\text{adj}(A)) = \det(A)^{n-1}$$

and

$$A \text{adj}(A) = \text{adj}(A) A = \det(A) I,$$

where  $I$  is the identity matrix.

**Theorem 2.1.** *Let  $A$ ,  $\mathbf{b}$  and  $m$  be as above. Then*

$$\eta(A, \mathbf{b}, m) \leq (\det(A), m)^n.$$

*If  $(\det(A), m) = 1$ , then  $\eta(A, \mathbf{b}, m) = 1$ .*

*Proof.* We multiply the congruence system  $A\mathbf{x} \equiv \mathbf{b} \pmod{m}$  with  $\text{adj}(A)$  and get

$$\begin{aligned} \text{adj}(A) A\mathbf{x} &\equiv \text{adj}(A) \mathbf{b} \pmod{m} \\ &\Leftrightarrow \\ \det(A) \mathbf{x} &\equiv \text{adj}(A) \mathbf{b} \pmod{m}, \end{aligned} \quad (3)$$

which is solvable if and only if  $\det(A)$  divides all elements in the vector  $\text{adj}(A)\mathbf{b}$ . If that is the case then this system has  $(\det(A), m)^n$  different solutions. If that

is not the case, then the original system has no solutions, since any solutions is also solutions to the rewritten system (3). When we multiply with  $\text{adj}(A)$  it might happen that we introduce new solutions. This proves that  $\eta(A, \mathbf{b}, m) \leq (\det(A), m)^n$ .

Assume that  $(\det(A), m) = 1$ . From (3) it follows that

$$\mathbf{x} \equiv \det(A)^{-1} \text{adj}(A) \mathbf{b} \pmod{m}$$

is a solution to the original system. Hence  $\eta(A, \mathbf{b}, m) = 1$ .  $\square$

**Theorem 2.2.** *Let  $A$ ,  $\mathbf{b}$  and  $m$  be as above. Assume that  $m = m_1 \cdots m_k$ , where the integers  $m_1, \dots, m_k$  are pairwise relatively prime. Then*

$$\eta(A, \mathbf{b}, m) = \eta(A, \mathbf{b}, m_1) \cdots \eta(A, \mathbf{b}, m_k).$$

Hence,  $\eta$  is multiplicative with respect to  $m$ .

*Proof.* If  $a \equiv b \pmod{m}$  and  $n$  divide  $m$ , then  $a \equiv b \pmod{n}$ . Hence any solution to  $A\mathbf{x} \equiv \mathbf{b} \pmod{m}$  is also a solution to every  $A\mathbf{x} \equiv \mathbf{b} \pmod{m_i}$ , where  $i = 1, 2, \dots, k$ . Assume that  $\mathbf{x}_i = (x_{i1}, x_{i2}, \dots, x_{in})$  is a solution to the congruence system  $A\mathbf{x} \equiv \mathbf{b} \pmod{m_i}$ , for  $i = 1, 2, \dots, k$ . Then for any  $k$ -tuple  $(\mathbf{x}_1, \mathbf{x}_2, \dots, \mathbf{x}_k)$  of solutions of the systems modulo  $m_i$  we construct a solution  $\mathbf{x} = (x_1, x_2, \dots, x_n)$  modulo  $m$ , by defining  $x_i$  to be the unique solution, due to the Chinese Remainder Theorem, modulo  $m$ , to the system

$$\begin{cases} x \equiv x_{1i} \pmod{m_1} \\ x \equiv x_{2i} \pmod{m_2} \\ \vdots \\ x \equiv x_{ki} \pmod{m_k}. \end{cases},$$

Since there are  $\eta(A, \mathbf{b}, m_1) \cdots \eta(A, \mathbf{b}, m_k)$  possible such  $k$ -tuples of solutions modulo  $m_i$ , the theorem follows (two different  $k$ -tuples can not generate the same solution modulo  $m$ ).  $\square$

### 3 Homogeneous Systems

We have already stated that we only have to consider congruence systems modulo a prime power. So, from now on  $m$  is going to be equal to  $p^k$ , where  $p$  is a prime number and  $k$  a positive integer. Let  $d = (A, p^k)$ , the greatest common divisor of all elements in the matrix  $A$  and the integer  $p^k$ , that is,

$$(A, p^k) = (a_{11}, a_{12}, \dots, a_{nn}, p^k).$$

Hence,  $d = p^e$  for some non-negative integer  $e \leq k$ .

**Lemma 3.1.** *Let  $d = (A, p^k)$  and let  $R = A/d$ . Then*

$$\eta(A, \mathbf{0}, p^k) = d^n \eta(R, \mathbf{0}, p^k/d).$$

Note that  $\eta(R, \mathbf{0}, 1) = 1$ .

*Proof.* Let  $\mathbf{x}'$  be a solution to  $R\mathbf{x} \equiv \mathbf{0} \pmod{p^k/d}$ . Note that  $\mathbf{x}'$  is also a solution to  $A\mathbf{x} \equiv \mathbf{0} \pmod{p^k}$ . This is also true for all elements on the form

$$\mathbf{x} = \mathbf{x}' + \frac{p^k}{d}\mathbf{u},$$

where  $\mathbf{u} \in \mathbb{Z}_d^n$ . This proves the theorem since  $|\mathbb{Z}_d^n| = d^n$ .  $\square$

Let  $p^l = p^k/d$  and let  $R$  be as in Lemma 3.1. We know that  $(R, p) = 1$  and therefore we can find some element in  $R$  that is relatively prime to  $p$ , say  $r_{11}$  after a possible rearrangement of rows and columns. Note that  $r_{11}$  is then invertible modulo  $p^l$ . By Gaussian elimination we get the equivalent system

$$\begin{cases} r_{11}x_1 + r_{12}x_2 + r_{13}x_3 + \cdots + r_{1n}x_n \equiv 0 \pmod{p^l} \\ r_{11}^{(1)}x_2 + r_{12}^{(1)}x_3 + \cdots + r_{1,n-1}^{(1)}x_n \equiv 0 \pmod{p^l} \\ \vdots \\ r_{n-1,1}^{(1)}x_2 + r_{n-1,2}^{(1)}x_3 + \cdots + r_{n-1,n-1}^{(1)}x_n \equiv 0 \pmod{p^l}, \end{cases} \quad (4)$$

where

$$r_{ij}^{(1)} \equiv r_{i+1,j+1} - r_{11}^{-1}r_{i+1,1}r_{1,j+1} \pmod{p^l}$$

for  $i, j = 1, 2, \dots, n-1$ . Let  $R^{(1)} = (r_{ij}^{(1)})$ . Hence,  $R^{(1)}$  is a square matrix of order  $n-1$ . Since  $r_{11}$  is invertible modulo  $p^l$  the two systems

$$R\mathbf{x} \equiv \mathbf{0} \pmod{p^l} \quad \text{and} \quad R^{(1)}\mathbf{x}^{(1)} \equiv \mathbf{0} \pmod{p^l}$$

has the same number of solutions. We have proved the first part of the following lemma.

**Lemma 3.2.** *With the notation above, we have*

$$\eta(R, \mathbf{0}, p^l) = \eta(R^{(1)}, \mathbf{0}, p^l). \quad (5)$$

Moreover, we have that  $(\det(R), p^l) = (\det(R^{(1)}), p^l)$ .

*Proof.* From the properties of the determinant it follows that

$$\det(R) \equiv r_{11}(-1)^{1+1} \det(R^{(1)}) \pmod{p^l}.$$

Since  $(r_{11}, p) = 1$  we have  $(\det(R), p^l) = (\det(R^{(1)}), p^l)$ .  $\square$

**Example 3.1.** Let  $p$  be a prime number,  $l$  a positive integer, and

$$R = \begin{pmatrix} r_{11} & r_{12} \\ r_{21} & r_{22} \end{pmatrix}$$

an integer matrix. Assume that  $(R, p) = (r_{11}, r_{12}, r_{21}, r_{22}, p) = 1$ . Consider the linear congruence system

$$\begin{cases} r_{11}x_1 + r_{12}x_2 \equiv 0 \pmod{p^l} \\ r_{21}x_1 + r_{22}x_2 \equiv 0 \pmod{p^l}. \end{cases} \quad (6)$$

Since  $(R, p) = 1$  one of the matrix entries must be relatively prime to  $p$ , assume that it is  $r_{11}$ . Let  $r_{11}^{-1}$  denote the multiplicative inverse of  $r_{11}$  modulo  $p^l$ . From the first congruence in the system (6) we have

$$x_1 \equiv -r_{11}^{-1}r_{12}x_2 \pmod{p^l}.$$

Hence,  $x_1$  is uniquely determined by  $x_2$  modulo  $p^l$ . By putting this expression for  $x_1$  in the second congruence in the system (6) we get

$$(r_{22} - r_{11}^{-1}r_{12}r_{21})x_2 \equiv 0 \pmod{p^l},$$

or equivalent

$$(r_{11}r_{22} - r_{12}r_{21})x_2 \equiv 0 \pmod{p^l}.$$

The coefficient for  $x_2$  is  $\det(R)$  and from the theory of linear congruences we know that this equation has  $(\det(R), p^l)$  incongruent solutions modulo  $p^l$ . We conclude that  $\eta(R, \mathbf{0}, p^l) = (\det(R), p^l)$ .

**Theorem 3.3.** *Let  $p$  be a prime number,  $l$  a positive integer, and  $A$  an integer square matrix of order  $n$ . Then*

$$\eta(A, \mathbf{0}, p^k) = p^{nk-\gamma}, \quad (7)$$

where  $\gamma = l_0 + l_1 + \dots + l_{n-1}$ . The numbers  $l_i$ , for  $i = 0, 1, \dots, n-1$ , are defined recursively in the following way:

$$p^{l_i} = \frac{p^{l_{i-1}}}{d_i}, \quad \text{and} \quad d_i = (R^{(i)}, p^{l_{i-1}}),$$

with  $d_0 = (A, p^k)$ ,  $p^{l_0} = p^k/d_0$  and where  $R^{(i)}$  is the matrix of order  $n-i$  given analogously as in (4) from  $R^{(i-1)}$ .

*Proof.* From Lemma 3.1 we have that

$$\eta(A, \mathbf{0}, p^k) = d_0^n \eta(R^{(0)}, \mathbf{0}, p^{l_0}),$$

where  $d_0 = (A, p^k)$  and  $p^{l_0} = p^k/d_0$ . If we now construct  $R^{(1)}$  from  $A/d_0$  in the same way as in the proof of Lemma 3.2 we get that

$$\eta(A, \mathbf{0}, p^k) = d_0^n \eta(R^{(1)}, \mathbf{0}, p^{l_0}).$$

We now do the same for the system  $R^{(1)}\mathbf{x} \equiv \mathbf{0} \pmod{p^{l_0}}$ . If  $R^{(1)} \equiv \mathbf{0} \pmod{p^{l_0}}$ , then  $\eta(R^{(1)}, \mathbf{0}, p^{l_0}) = p^{l_0(n-1)}$  and in this case  $\gamma = l_0$ . Otherwise, we construct the matrix  $R^{(2)}$  of order  $n-2$  from  $R^{(1)}$  in the same way as we constructed  $R^{(1)}$  before. Let  $d_1 = (R^{(1)}, p^{l_0})$  and  $p^{l_1} = p^{l_0}/d_1$ . By using Lemma 3.1 and Lemma 3.2 again we get

$$\eta(A, \mathbf{0}, p^k) = d_0^n d_1^{n-1} \eta(R^{(2)}, \mathbf{0}, p^{l_1}).$$

If  $R^{(2)} \equiv \mathbf{0} \pmod{p^{l_1}}$  then  $\eta(R^{(2)}, \mathbf{0}, p^{l_1}) = p^{l_1}$  and  $\gamma = l_0 + l_1$ . If we continue in this way we get

$$\eta(A, \mathbf{0}, p^k) = d_0^n d_1^{n-1} \dots d_{n-2}^2 \eta(R^{(n-1)}, \mathbf{0}, p^{l_{n-2}}).$$

The matrix  $R^{(n-1)}$  is of order 1, that is, a single integer  $r_{11}^{(n-1)}$ . Let

$$d_{n-1} = (R^{(n-1)}, p^{n-2}) = (r_{11}^{(n-1)}, p^{l_{n-2}}) \quad \text{and} \quad p^{l_{n-1}} = p^{l_{n-2}}/d_{n-1}.$$

The congruence  $R^{(n-1)}\mathbf{x} \equiv \mathbf{0} \pmod{p^{l_{n-2}}}$  is equivalent to

$$r_{11}^{(n-1)}x \equiv 0 \pmod{p^{l_{n-2}}},$$

which have  $d_{n-1}$  incongruent solutions modulo  $p^{l_{n-2}}$ . Hence

$$\eta(R^{(n-1)}, \mathbf{0}, p^{l_{n-2}}) = d_{n-1}.$$

We have showed that

$$\eta(A, \mathbf{0}, p^k) = d_0^n d_1^{n-1} \cdots d_{n-2}^2 d_{n-1}.$$

Let  $l_{-1} = k$ . From  $d_t = p^{l_{t-1}}/p^{l_t} = p^{l_{t-1}-l_t}$  it follows that

$$d_0^n d_1^{n-1} \cdots d_{n-2}^2 d_{n-1} = \prod_{i=0}^{n-1} p^{(n-i)(l_{i-1}-l_i)} = p^{nk} \prod_{i=0}^{n-1} p^{-l_i} = p^{nk-\gamma},$$

since  $\gamma = l_0 + l_1 + \cdots + l_{n-1}$ . This proves that  $\eta(A, \mathbf{0}, p^k) = p^{nk-\gamma}$ .  $\square$

**Theorem 3.4.** *With the same notations as above,  $(\det(A), p^{nk}) = p^{nk-\gamma}$ .*

*Proof.* Let  $R^{(0)} = A$ ,  $d_0 = (R^{(0)}, p^k)$ ,  $d_i = (R^{(i)}, p^{l_{j-1}})$ , where  $R^{(i)}$  is constructed as above. Let also  $S^{(i)} = R^{(i)}/d_i$ . Hence  $R^{(i+1)}$  is the submatrix we get from Gaussian elimination in  $S^{(i)}$  by excluding the first row and column. It is clear that

$$\det(A) = \det(R^{(0)}) = d_0^n \det(S^{(0)}).$$

After Gaussian elimination and expansion along the first column we have

$$\det(S^{(0)}) \equiv \det(R^{(1)}) \pmod{p^{l_0}}$$

and

$$(\det(S^{(0)}), p^{l_0}) = (\det(R^{(1)}), p^{l_0}).$$

Hence,

$$(\det(A), d_0^n p^{l_0}) = (\det(S^{(0)})d_0^n, d_0^n p^{l_0}) = (\det(R^{(1)})d_0^n, d_0^n p^{l_0}).$$

Observe that  $d_0^n p^{l_0} = p^{nk-(n-1)l_0}$ . In general we have

$$\det(R^{(j)}) = d_j^{n-j} \det(S^{(j)})$$

and

$$(\det(S^{(j)}), p^{l_j}) = (\det(R^{(j+1)}), p^{l_j}),$$

for  $j = 0, 1, \dots, n-1$ . By induction

$$(\det(A), d_0^n \cdots d_{j-1}^{n-j+1} p^{l_j}) = (\det(R^{(j)})d_0^n \cdots d_{j-1}^{n-j+1}, d_0^n \cdots d_{j-1}^{n-j+1} p^{l_j}),$$

for all  $j$ . For  $j = n - 1$  we get

$$\begin{aligned} (\det(A), d_0^n \cdots d_{n-2}^2 p^{l_{n-2}}) &= (\det(R^{(n-1)}) d_0^n \cdots d_{n-2}^2, d_0^n \cdots d_{n-2}^2 p^{l_{n-2}}) \\ &= d_0^n \cdots d_{n-2}^2 (\det(R^{(n-1)}), p^{l_{n-2}}) = d_0^n \cdots d_{n-1} = p^{nk-\gamma}. \end{aligned}$$

Since  $p^{nk} \geq d_0^n \cdots d_{n-2}^2 p^{l_{n-2}} \geq p^{nk-\gamma}$  we conclude

$$(\det(A), p^{nk}) = p^{nk-\gamma}. \quad \square$$

**Corollary 3.5.** *The number of solutions of  $A\mathbf{x} \equiv \mathbf{0} \pmod{p^k}$  is*

$$\eta(A, \mathbf{0}, p^k) = (\det(A), p^{nk}).$$

**Theorem 3.6.** *Let  $A$  be a square integer matrix of order  $n$ , and  $m$  a positive integer. Assume that  $m = \prod_{i=1}^N p_i^{k_i}$ , where  $p_i$  are different primes. Then*

$$\eta(A, \mathbf{0}, m) = m^n \prod_{i=1}^N p_i^{-\gamma_i} = (\det(A), m^n)$$

where  $\gamma_i$  is defined as in Theorem 3.3.

*Proof.* This is a direct consequence of Theorem 2.2 and Theorem 3.3  $\square$

From Theorem 2.1 and Theorem 3.6 we have

$$\eta(A, \mathbf{0}, m) = (\det(A), m^n) \leq (\det(A), m)^n$$

and with equality when  $(\det(A), m)^n \mid \det(A)$ .

## 4 Inhomogeneous Systems

**Theorem 4.1.** *Let  $p$  be a prime number,  $k$  a positive integer,  $A$  be a square integer matrix of order  $n$ , and  $\mathbf{b}$  an integer vector of length  $n$ . The inhomogeneous linear system*

$$A\mathbf{x} \equiv \mathbf{b} \pmod{p^k} \quad (8)$$

*is solvable if and only if  $d_0 \mid \mathbf{b}$  and  $d_j \mid \mathbf{b}^{(j)}$  for all  $0 \leq j \leq n-1$ , where the integers  $d_j$  are given in similar way as in Theorem 3.3 and the vectors  $\mathbf{b}^{(j)}$  is the last  $n-j$  elements in the right hand side of the system after the  $j$ th step of the Gaussian elimination. Moreover, if the system is solvable then*

$$\eta(A, \mathbf{b}, p^k) = \eta(A, \mathbf{0}, p^k) = p^{nk-\gamma} = (\det(A), p^{nk}).$$

*Proof.* Let  $d_0 = (\det(A), p^k)$ . The system (8) is solvable when  $d_0$  divide each component of  $\mathbf{b}$ . Let  $R^{(0)} = A/d_0$  and  $\mathbf{b}^{(0)} = \mathbf{b}/d_0$ . Reduce the system in the same way as in Lemma 3.2, the first step in the Gaussian elimination. We get the inhomogeneous system

$$R^{(1)}\mathbf{x}^{(1)} \equiv \mathbf{b}^{(1)} \pmod{p^{l_0}},$$

with  $n - 1$  unknowns and where

$$b_i^{(1)} \equiv b_i^{(0)} - b_1^{(0)} r_{i,1}^{(0)} (r_{11}^{(0)})^{-1} \pmod{p^{l_0}} \quad \text{for } i = 2, 3, \dots, n.$$

In order for this system to have solutions  $d_1 = (R^{(1)}, p^{l_0})$  must divide all the components of  $\mathbf{b}^{(1)}$ . If we continue in this way we get that (8) is solvable if and only if  $d_0 \mid \mathbf{b}$  and  $d_j \mid \mathbf{b}^{(j)}$  for all  $0 \leq j \leq n - 1$ . The number of solutions, if they exists, are the same as in homogeneous case—the backward substitution result in the same number of solutions in each step.  $\square$

## 5 Algorithm

Let  $p$  be a prime number,  $n$  and  $k$  positive integers,  $A = (a_{ij})_{n \times n}$  an integer matrix, and  $\mathbf{b} = (b_i)_{n \times 1}$  a vector with integer entries. The following algorithm decides if the congruence

$$A\mathbf{x} \equiv \mathbf{b} \pmod{p^k}$$

is solvable, and in that case find the number of solutions, denoted  $\eta$ , and the set  $X$  of all solutions. In the algorithm we will work with matrices on the block matrix form

$$A^{(t)} = \begin{pmatrix} a_{ij}^{(t)} & \\ & 0 \end{pmatrix}_{n \times n} = \begin{pmatrix} U^{(t)} & B^{(t)} \\ 0 & R^{(t)} \end{pmatrix}, \quad t = 1, 2, \dots, n - 1,$$

where  $U^{(t)}$  is an upper triangular square matrix of order  $t$ ,  $B^{(t)}$  is a  $t \times n - t$  matrix,  $0$  is the zero matrix of type  $(n - t) \times t$ , and  $R^{(t)}$  is a square matrix of order  $n - t$ . Let  $R^{(0)} = A^{(0)}$ . Hence,  $A^{(n-1)}$  is an upper triangular matrix. Let  $r_{ij}^{(t)}$  denote the element on the  $i$ th row and the  $j$ th column in  $R^{(t)}$ . Then

$$r_{ij}^{(t)} = a_{t+i, t+j}^{(t)}.$$

Let  $b_i^{(t)}$  denote the  $i$ th element in the vector  $\mathbf{b}^{(t)}$ . Set

$$\mathbf{r}^{(t)} = (b_{t+1}^{(t)}, b_{t+2}^{(t)}, \dots, b_n^{(t)}),$$

that is, the  $n - t$  last elements in  $\mathbf{b}^{(t)}$ . Hence,  $\mathbf{r}^{(0)} = \mathbf{b}^{(0)}$ . Note that when we change  $R^{(t)}$  or  $\mathbf{r}^{(t)}$  we also change  $A^{(t)}$  and  $\mathbf{b}^{(t)}$ , respectively. Let  $U(q, n) = \mathbb{Z}_q^n$ .

### 1. INITIALIZAION

- 1.1.  $l_{-1} \leftarrow k$
- 1.2.  $\sigma \leftarrow \text{id}$ , the permutation which represent the interchanges of columns
- 1.3.  $d_0 \leftarrow (A, p^k)$ , note that  $d_0 = p^{e_0}$  for some integer  $e_0$
- 1.4.  $l_0 \leftarrow k - e_0$ , that is  $p^{l_0} = p^k / d_0$
- 1.5.  $\gamma \leftarrow l_0$
- 1.6.  $A^{(0)} \leftarrow A / d_0$



- 1.7. If  $d_0 \mid \mathbf{b}$ , then  $\mathbf{b}^{(0)} \leftarrow \mathbf{b}/d_0$ , else goto step 5
- 1.8. If  $d_0 = p^k$ , then  $X \leftarrow U(p^k, n)$  and goto step 4, note that  $\gamma = 0$

## 2. GAUSSIAN ELIMINATION

For  $t = 1, 2, \dots, n-1$  do

- 2.1. Find  $u$  and  $v$  such that  $(r_{uv}^{(t-1)}, p) = 1$
- 2.2. Interchange  $t$ th and  $(t+u-1)$ th row, and  $t$ th and  $(t+v-1)$ th column of  $A^{(t-1)}$ . Let  $A^{(t)}$  denote the new matrix.
- 2.3. Interchange  $t$ th and  $(t+u-1)$ th elements of  $\mathbf{b}^{(t-1)}$ . Let  $\mathbf{b}^{(t)}$  denote the new vector.
- 2.4. Swap:  $\sigma(t) \leftarrow \sigma(t+v-1)$  and  $\sigma(t+v-1) \leftarrow \sigma(t)$
- 2.5. For  $i, j = t+1, t+2, \dots, n$  do
  - 2.5.1.  $a_{ij}^{(t)} \leftarrow a_{ij}^{(t)} - (a_{tt}^{(t)})^{-1} a_{it}^{(t)} a_{tj}^{(t)} \bmod p^{l_{t-1}}$
  - 2.5.2.  $b_i^{(t)} \leftarrow b_i^{(t)} - (a_{tt}^{(t)})^{-1} a_{it}^{(t)} b_t^{(t)} \bmod p^{l_{t-1}}$
  - 2.5.3.  $a_{it}^{(t)} \leftarrow 0$
- 2.6.  $d_t \leftarrow (R^{(t)}, p^{l_{t-1}})$ , note that  $d_t = p^{e_t}$  for some integer  $e_t$
- 2.7.  $l_t \leftarrow l_{t-1} - e_t$ , that is  $p^{l_t} = p^{l_{t-1}}/d_t$
- 2.8.  $\gamma \leftarrow \gamma + l_t$
- 2.9.  $R^{(t)} \leftarrow R^{(t)}/d_t$
- 2.10. If  $d_t \mid \mathbf{r}^{(t)}$ , then  $\mathbf{r}^{(t)} \leftarrow \mathbf{r}^{(t)}/d_t$ , else goto step 5
- 2.11. If  $d_t = p^{l_{t-1}}$ , then  $X \leftarrow U(p^{l_{t-1}}, n-t)$  and goto step 3
- 2.12. If  $t = n-1$ , then
  - 2.12.1.  $x_n \leftarrow (a_{nn}^{(n-1)})^{-1} b_n \bmod p^{l_{n-1}}$
  - 2.12.2.  $X \leftarrow x_n + p^{l_{n-1}} U(d_{n-1}, 1) \bmod p^{l_{n-2}}$

## 3. BACKWARD SUBSTITUTION

For  $s = t, t-1, \dots, 1$  do

- 3.1  $Y \leftarrow \emptyset$
- 3.2 For each  $\mathbf{x} = (x_{s+1}, x_{s+2}, \dots, x_n) \in X$  do
  - 3.2.1  $x_s \leftarrow (a_{ss}^{(t)})^{-1} \left( b_s^{(t)} - \sum_{j=s+1}^n a_{sj}^{(t)} x_j \right) \bmod p^{l_{s-1}}$
  - 3.2.2  $\mathbf{x} \leftarrow (x_s, x_{s+1}, \dots, x_n)$ , that is, prepend  $x_s$  to  $\mathbf{x}$
  - 3.2.3  $Y \leftarrow Y \cup (\mathbf{x} + p^{l_{s-1}} U(d_{s-1}, n-s+1) \bmod p^{l_{s-2}})$
- 3.3  $X \leftarrow Y$

## 4. SOLVABLE

- 4.1. For each  $\mathbf{x} = (x_1, x_2, \dots, x_n) \in X$  do  $\mathbf{x} \leftarrow (x_{\sigma(1)}, x_{\sigma(2)}, \dots, x_{\sigma(n)})$
- 4.2.  $\eta \leftarrow p^{nk-\gamma}$
- 4.3. Goto step 6

## 5. NOT SOLVABLE

5.1.  $\eta \leftarrow 0$

5.2.  $X \leftarrow \emptyset$

## 6. OUTPUT AND FINISH

6.1. Return  $\eta$  and  $X$

**Remark.** After step 1.7: we have transformed

$$A\mathbf{x} \equiv \mathbf{b} \pmod{p^k} \quad \text{to} \quad A^{(0)}\mathbf{x} \equiv \mathbf{b}^{(0)} \pmod{p^{l_0}}.$$

After step 2.10: we have transformed

$$R^{(t)}\mathbf{x} \equiv \mathbf{r}^{(t)} \pmod{p^{l_{t-1}}} \quad \text{to} \quad R^{(t)}\mathbf{x} \equiv \mathbf{r}^{(t)} \pmod{p^{l_t}}$$

since  $p^{l_t} = p^{l_{t-1}}/d_t$ . During the backward substitution solve first modulo  $p^{l_t}$  and thereafter lift to modulo  $p^{l_{t-1}}$ .

**Remark.** If we are only interested in finding the number of solutions its preferable to use the formula with the determinant.

**Example 5.1.** Study the linear congruence system

$$\begin{cases} 123x_1 + 152x_2 + 28x_3 + 22x_4 + 144x_5 \equiv 193 \\ 38x_1 + 189x_2 + 127x_3 + 171x_4 + 141x_5 \equiv 2 \\ 132x_1 + 232x_2 + 215x_3 + 22x_4 \equiv 96 \\ 155x_1 + 30x_2 + 178x_3 + 142x_4 + 127x_5 \equiv 198 \\ 194x_1 + 171x_2 + 16x_3 + 24x_4 + 98x_5 \equiv 162 \end{cases} \pmod{3^5},$$

where  $3^5 = 243$ . Any solutions are elements in the set

$$X \subseteq U = \mathbb{Z}_{243} \times \mathbb{Z}_{243} \times \mathbb{Z}_{243} \times \mathbb{Z}_{243} \times \mathbb{Z}_{243}.$$

Let

$$A = \begin{pmatrix} 123 & 152 & 28 & 22 & 144 \\ 38 & 189 & 127 & 171 & 141 \\ 132 & 232 & 215 & 22 & 0 \\ 155 & 30 & 178 & 142 & 127 \\ 194 & 171 & 16 & 24 & 98 \end{pmatrix} \quad \text{and} \quad \mathbf{b} = \begin{pmatrix} 193 \\ 2 \\ 96 \\ 198 \\ 162 \end{pmatrix}.$$

Set  $l_{-1} = 5$ . We have that  $e_0 = 0$ ,  $d_0 = 1$ ,  $l_0 = 5$ , and  $\gamma = l_0 = 5$ . Initial we let

$$\sigma = \text{id} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix}.$$

Since  $d_0 = 0$ , we have that  $A^{(0)} = A$  and  $\mathbf{b}^{(0)} = \mathbf{b}$ . Note that  $R^{(0)} = A^{(0)}$ . We interchange row 1 and 2. After the first step in the Gaussian elimination we get

$$A^{(1)} = \begin{pmatrix} 38 & 189 & 127 & 171 & 141 \\ 0 & 71 & 7 & 76 & 180 \\ 0 & 151 & 68 & 157 & 9 \\ 0 & 84 & 114 & 52 & 121 \\ 0 & 63 & 135 & 123 & 56 \end{pmatrix} \quad \text{and} \quad \mathbf{b}^{(1)} = \begin{pmatrix} 2 \\ 97 \\ 153 \\ 241 \\ 139 \end{pmatrix}.$$

The system given by the matrix  $A^{(1)}$  and vector  $\mathbf{b}^{(1)}$  have the same solutions as original system. Further, the new system have as many solutions as

$$R^{(1)}\mathbf{x} \equiv \mathbf{r}^{(1)} \pmod{3^5},$$

where

$$R^{(1)} = \begin{pmatrix} 71 & 7 & 76 & 180 \\ 151 & 68 & 157 & 9 \\ 84 & 114 & 52 & 121 \\ 63 & 135 & 123 & 56 \end{pmatrix} \quad \text{and} \quad \mathbf{r}^{(1)} = \begin{pmatrix} 97 \\ 153 \\ 241 \\ 139 \end{pmatrix}.$$

For this system we find that  $e_1 = 0$ ,  $d_1 = 1$ ,  $l_1 = 5$ , and  $\gamma = l_0 + l_2 = 10$ . One more step with the Gaussian elimination results in

$$A^{(2)} = \begin{pmatrix} 38 & 189 & 127 & 171 & 141 \\ 0 & 71 & 7 & 76 & 180 \\ 0 & 0 & 36 & 122 & 54 \\ 0 & 0 & 27 & 10 & 175 \\ 0 & 0 & 9 & 213 & 218 \end{pmatrix} \quad \text{and} \quad \mathbf{b}^{(2)} = \begin{pmatrix} 2 \\ 97 \\ 22 \\ 181 \\ 94 \end{pmatrix}.$$

Next we have to interchange column 3 and 4 since none of 36, 27 or 9 are relative prime to 3. Hence, the column permutations is so far given by

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 4 & 3 & 5 \end{pmatrix}.$$

We get that  $e_2 = 0$ ,  $d_2 = 1$ ,  $l_2 = 5$ , and  $\gamma = l_0 + l_1 + l_2 = 15$ . The next step in the Gaussian elimination gives us that

$$A^{(3)} = \begin{pmatrix} 38 & 189 & 171 & 127 & 141 \\ 0 & 71 & 76 & 7 & 180 \\ 0 & 0 & 122 & 36 & 54 \\ 0 & 0 & 0 & 36 & 67 \\ 0 & 0 & 0 & 225 & 56 \end{pmatrix} \quad \text{and} \quad \mathbf{b}^{(3)} = \begin{pmatrix} 2 \\ 97 \\ 22 \\ 227 \\ 199 \end{pmatrix}.$$

Again, we have to interchange columns since both 36 and 225 are not relative prime to 3. That gives us the column permutation

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 4 & 3 & 5 \end{pmatrix}.$$

After the last step in the Gaussian elimination we have that

$$\begin{pmatrix} 38 & 189 & 171 & 141 & 127 \\ 0 & 71 & 76 & 180 & 7 \\ 0 & 0 & 122 & 54 & 36 \\ 0 & 0 & 0 & 67 & 36 \\ 0 & 0 & 0 & 0 & 126 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 2 \\ 97 \\ 22 \\ 227 \\ 216 \end{pmatrix},$$

and  $e_3 = 0$ ,  $d_3 = 1$ ,  $l_3 = 5$ , and  $\gamma = l_0 + l_1 + l_2 + l_3 = 20$ . Finally, we get that  $e_4 = 2$ ,  $d_4 = 9$ ,  $l_4 = 3$ , and  $\gamma = l_0 + l_1 + l_2 + l_3 + l_4 = 23$ . Since  $d_4 = 2^2 = 9$  divide both 126 and 216, the system is solvable, and we have that

$$A^{(4)} = \begin{pmatrix} 38 & 189 & 171 & 141 & 127 \\ 0 & 71 & 76 & 180 & 7 \\ 0 & 0 & 122 & 54 & 36 \\ 0 & 0 & 0 & 67 & 36 \\ 0 & 0 & 0 & 0 & 14 \end{pmatrix} \quad \text{and} \quad \mathbf{b}^{(4)} = \begin{pmatrix} 2 \\ 97 \\ 22 \\ 227 \\ 24 \end{pmatrix}.$$

Now, we do backward substitution on the linear congruence system

$$\begin{cases} 38y_1 + 189y_2 + 171y_3 + 141y_4 + 127y_5 \equiv 2 \pmod{3^5} \\ 71y_2 + 76y_3 + 180y_4 + 7y_5 \equiv 97 \pmod{3^5} \\ 122y_3 + 54y_4 + 36y_5 \equiv 22 \pmod{3^5} \\ 67y_4 + 36y_5 \equiv 227 \pmod{3^5} \\ 14y_5 \equiv 24 \pmod{3^3}, \end{cases} \quad (9)$$

where

$$\begin{cases} 38^{-1} \equiv 32 \pmod{3^5} \\ 71^{-1} \equiv 89 \pmod{3^5} \\ 122^{-1} \equiv 2 \pmod{3^5} \\ 67^{-1} \equiv 214 \pmod{3^5} \\ 14^{-1} \equiv 2 \pmod{3^3} \end{cases} \quad \text{and} \quad \begin{cases} x_1 = y_{\sigma(1)} = y_1 \\ x_2 = y_{\sigma(2)} = y_2 \\ x_3 = y_{\sigma(3)} = y_4 \\ x_4 = y_{\sigma(4)} = y_5 \\ x_5 = y_{\sigma(5)} = y_3. \end{cases}$$

Before we find the solutions we conclude that the number of solution is

$$p^{nk-\gamma} = 3^{5 \cdot 5 - 23} = 3^2 = 9.$$

First we have that

$$x_4 = y_5 \equiv 2 \cdot 24 \equiv 21 \pmod{3^3}.$$

We lift the result to  $\mathbb{Z}_{243}$ , that is,

$$x_4 = y_5 = 21 + 3^4 h = 21 + 3^3 h, \quad h \in \mathbb{Z}_{d_4} = \mathbb{Z}_9.$$

Hence,  $x_4 \in \{21, 48, 75, 102, 129, 156, 183, 210, 237\}$ . Since 36 is divisible by 9, neither  $y_4$  or  $y_3$  depends on  $y_4$ , which follows from

$$36 \cdot (21 + 3^3 h) \equiv 36 \cdot 21 \equiv 27 \pmod{3^5}.$$

We get that  $x_5 = y_4 = 179$  and  $x_3 = y_5 = 32$ . The two first congruences in the system (9) gives us the nine solutions:

$$\begin{array}{lll} (43, 127, 32, 21, 179) & (151, 73, 32, 48, 179) & (16, 19, 32, 75, 179) \\ (124, 208, 32, 102, 179) & (232, 154, 32, 129, 179) & (97, 100, 32, 156, 179) \\ (205, 46, 32, 183, 179) & (70, 235, 32, 210, 179) & (178, 181, 32, 237, 179). \end{array}$$

## 6 Discussion

In this paper we made the choice to you use as elementary methods as possible. Mainly because the problem is of an elementary nature but also because of the interest from applications. It is possible to lift both the problem and its solution into the context of free modules, see [5], over the ring  $\mathbb{Z}/m\mathbb{Z}$ . The derivation will when be almost identical but with different vocabulary.

By small changes it is also possible to solve system of congruence equations with different modulus. We construct a system modulo the least common multiple of all the moduli, that are equivalent to the original system. This is the same technique that is mentioned in [1].

## References

- [1] A.T. Butson, B.M. Stewart, *Systems of linear congruences*, Canad. J. Math. 7, pages 358–368, 1955.
- [2] J. Cullen, *The Solutions of a Systems of Linear Congruences*, Proc. London Math. Soc., volume s1–34, pages 323–346, 1901.
- [3] Andreas Dolzmann and Thomas Sturm, *Solving Systems of Linear Congruences*, [citeseer.ist.psu.edu/669451.html](http://citeseer.ist.psu.edu/669451.html), 2001.
- [4] Andreas Dolzmann and Thomas Sturm, *Parametric Systems of Linear Congruences* in *Computer Algebra in Scientific Computing. Proceedings of the CASC 2001*, Viktor G. Ganzha, Ernst W. Mayr and Evgenii V. Vorozhtsov (editors), pages 149–166, Springer, Berlin, 2001.
- [5] Serge Lang, *Algebra*, Springer Verlag, 2004.
- [6] P. J. McCarthy, *The Number of Restricted Solutions of some Systems of Linear Congruences*, Rendiconti del Seminario Matematico della Università di Padova, 54 (1975), pages 59–68.
- [7] Marcus Nilsson and Robert Nyqvist, *On monomial dynamical systems on the  $p$ -adic torus*, Contemporary Mathematics 508, pages 121–132, AMS, 2010.
- [8] Kenneth H. Rosen, *Elementary Number Theory and Its Applications*, Pearson, 2011.
- [9] Florentin Smarandachw, *Algorithms For Solving Linear Congruences ans Systems of Linear Congruences*, [arXiv:math/0702488v1](https://arxiv.org/abs/math/0702488v1) [math.GM], 1987.